INCLUDES

NEWNES ONLINE MEMBERSHIP

RF & WIRELESS TECHNOLOGIES

know it all

- A 360 degree view from our best-selling authors
- Hot topics covered including ultrawideband and cognitive radio technologies
- The ultimate hard-working desk reference: all the essential information, techniques, and tricks of the trade in one volume

Fette • Aiello • Chandra • Dobkin • Bensky
Miron • Lide • Dowla • Olexa

RF & Wireless Technologies

Newnes Know It All Series

PIC Microcontrollers: Know It All
Lucio Di Jasio, Tim Wilmshurst, Dogan Ibrahim, John Morton,
Martin Bates, Jack Smith, D.W. Smith, and Chuck Hellebuyck
ISBN: 978-0-7506-8615-0

Embedded Software: Know It All
Jean Labrosse, Jack Ganssle, Tammy Noergaard, Robert Oshana, Colin Walls, Keith Curtis,
Jason Andrews, David J. Katz, Rick Gentile, Kamal Hyder, and Bob Perrin
ISBN: 978-0-7506-8583-2

Embedded Hardware: Know It All
Jack Ganssle, Tammy Noergaard, Fred Eady, Creed Huddleston, Lewin Edwards,
David J. Katz, Rick Gentile, Ken Arnold, Kamal Hyder, and Bob Perrin
ISBN: 978-0-7506-8584-9

Wireless Networking: Know It All
Praphul Chandra, Daniel M. Dobkin, Alan Bensky, Ron Olexa,
David A. Lide, and Farid Dowla
ISBN: 978-0-7506-8582-5

RF & Wireless Technologies: Know It All
Bruce Fette, Roberto Aiello, Praphul Chandra, Daniel M. Dobkin,
Alan Bensky, Douglas Miron, David A. Lide, Farid Dowla, and Ron Olexa
ISBN: 978-0-7506-8581-8

For more information on these and other Newnes titles visit: www.newnespress.com

RF & Wireless Technologies

Bruce Fette
Roberto Aiello
Praphul Chandra
Daniel M. Dobkin
Alan Bensky
Douglas Miron
David A. Lide
Farid Dowla
Ron Olexa

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Newnes is an imprint of Elsevier

Newnes is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Library of Congress Cataloging-in-Publication Data
Application submitted

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-0-7506-8581-8

Typeset by Charon Tec Ltd (A Macmillan Company), Chennai, India
www.charontec.com
Printed in the United States of America

07 08 09 10 10 9 8 7 6 5 4 3 2 1

Cover image by iStockphoto

Contents

About the Authors

Hong Jo Ahn (Chapter 30) was a contributor to *Handbook of RF & Wireless Technologies*. Ahn is associated with the Analog VLSI Laboratory of the Ohio State University in Columbus, Ohio.

Roberto Aiello (Chapter 21) is the editor of *Ultra Wideband Systems*. Dr. Aiello is the founding CEO and now CTO of Staccato Communications. Prior to working at Staccato, he was founder, president, and CEO of Fantasma Networks, an ultra wideband (UWB) product company. Previously, Dr. Aiello led the wireless research and built the first documented UWB network at Interval Research, Paul Allen's research laboratory. Earlier, he held senior positions at the Stanford Linear Accelerator Center and the National Superconducting Super Collider Laboratory in Texas. Dr. Aiello is a recognized leader in the UWB community, and his efforts were instrumental in getting UWB spectrum allocated in the United States. Dr. Aiello holds a PhD in physics from the University of Trieste. He serves on several advisory boards and is the author of more than 20 patents on UWB technology.

Adem Aktasa (Chapter 30) was a contributor to *Handbook of RF & Wireless Technologies*. Aktasa is associated with the Analog VLSI Laboratory of the Ohio State University in Columbus, Ohio.

The Automatic Identification Manufacturers (AIM) Organization (Chapter 19) was a contributor to *Handbook of RF & Wireless Technologies*. AIM is a radio frequency identification (RFID) industry group based in Pittsburgh, PA.

Alan Bensky, MScEE (Chapters 2, 3, 4, and 5) is an electronics engineering consultant with over 25 years of experience in analog and digital design, management, and marketing. Specializing in wireless circuits and systems, Bensky has carried out projects for varied military and consumer applications. He is the author of *Short-range Wireless Communication, Second Edition*, published by Elsevier, 2004, and has written several articles in international and local publications. He has taught courses and gives lectures on radio engineering topics. Bensky is a senior member of IEEE.

Brad Brannon (Chapter 18) was a contributor to *Handbook of RF & Wireless Technologies*. He is an engineer with Analog Devices in Greensboro, NC.

Praphul Chandra (Chapters 10 and 11) works as a Research Scientist at HP Labs, India in the Access Devices Group. He joined HP Labs in April 2006. Prior to joining HP he was a senior design engineer at Texas Instruments (USA) where he worked on Voice over IP with specific focus on Wireless Local Area Networks. He is the author of two books—*Bulletproof Wireless Security* and *Wi-Fi Telephony: Challenges and Solutions for Voice over WLANs*. He is an Electrical Engineer by training, though his interest in social science and politics has prompted him to concurrently explore the field of Public Policy. He maintains his personal website at www.thecofi.net.

Daniel M. Dobkin (Chapters 8 and 9) is the author of *RF Engineering for Wireless Networks*. He has been involved in the design, fabrication, and characterization of devices and systems used in microwave wireless communications for over two decades. He is currently an independent consultant involved in research and teaching related to RFID and other fields in communications. He has taught numerous introductory short courses in RFID technology in the United States and Singapore. Dr. Dobkin received his PhD degree from Stanford University in 1985 and his B.S. from the California Institute of Technology in 1976. He is the author of about 30 technical publications, inventor or co-inventor of six U.S. patents, and has written two technical books: Principles of Chemical Vapor Deposition with Michael Zuraw and RF Engineering for Wireless Networks.

Farid Dowla (Chapters 1, 14, 15, 16, 17, 18, 19) is the editor of *Handbook of RF & Wireless Technologies*. Dowla received his BS, MS, and PhD in electrical engineering from the Massachusetts Institute of Technology. He joined Lawrence Livermore National Laboratory shortly after receiving his doctorate in 1985. His research interests include adaptive filters, signal processing, wireless communication systems, and RF/mobile communication. He currently directs a research team focused on ultra-widebandRFradar and communication systems. Dowla is also an adjunct associate professor of electrical engineering at the University of California at Davis. He is a member of the Institute of Electrical and Electronic Engineers (IEEE) and Sigma Xi. He holds three patents in the signal processing area, has authored a book on neural networks for the U.S. Department of Defense, and has edited a book on geophysical signal processing. He contributes to numerous IEEE and professional journals and is a frequent seminar participant at professional conferences.

Bruce A. Fette, Ph.D. (Chapters 24 and 25) is the Editor of *Cognitive Radio Technology*. He is chief scientist for Communications Networks business area of General Dynamics C4 Systems. He has been with the company for over 38 years, specializing in advanced signal processing technology and systems for telephone and radio frequency communications. With 35 patents to his credit, Dr. Fette has been responsible for many of the enabling technologies leading to today's advanced communication products and systems. He earned his BSEE from the University of Cincinnati in 1969, his MSEE and doctorate from Arizona State University in 1974 and 1981 respectively. In addition to his many roles with the SDR Forum, Dr. Fette is also an active member of IEEE.

Mohammed Ismail (Chapter 30) was a contributor to *Handbook of RF & Wireless Technologies*. He is a professor of electrical engineering at the Ohio State University in Columbus, Ohio.

Michael LeFevre (Chapter 29) was a contributor to *Handbook of RF & Wireless Technologies*. LeFevre received his MS in electrical engineering from Brigham Young University in 1997. He is currently a Systems Engineer with the RF & DSP Infrastructure Division of the Motorola Semiconductor Products Sector in Tempe, Arizona.

David A. Lide (Chapter 10) is the author of *Wi-Fi Telephony*. He currently is a Senior Member of the Technical Staff at Texas Instruments and has worked on various aspects of Voice over IP for the past nine years. Prior to that, he has worked on Cable Modem design and on weather satellite ground systems. He lives with his family in Rockville, Maryland.

Preston Marshall (Chapter 27) was a contributor to *Cognitive Radio Technolgy*. He has 30 years of experience in communications and software and hardware system development. Currently he is a Program Manager with the Defense Advanced Research Projects Agency (DARPA) Strategic Technology Office (STO). Mr. Marshall is responsible for and manages several of the DARPA Networking programs. These programs are:

Connectionless Networking, which investigates low energy protocols in low duty cycle ad-hoc networks; neXt Generation (XG) Communications, focusing on the development of networks that provide adaptive spectrum usage; WOLFPACK, developing a distributed network of forward positioned, Coke-can sized electronic and network warfare devices; Disruption Tolerant Networking, developing delay tolerant networking and extending existing technology to address episodic connectivity, distributed name and routing spaces, and non-IP system transport; and a program to develop very small radioisotope power sources. Before his assignment to DARPA's Strategic Technology Office, Mr. Marshall was employed by a number of systems and electronics companies. Mr. Marshall holds a BSEE and M.S. Information Science from Lehigh University.

Earl McCune (Chapter 28) was a contributor to *Handbook of RF & Wireless Technologies*. He is chief technical officer and co-founder of Tropian, Inc. in Cupertino, Calif. He received his BS/EECS degree from the University of California at Berkeley; his MS from Stanford University; and his PhD from the University of California at Davis. McCune has more than 20 years of experience with creating and managing the creation of new technologies for wireless communications. McCune founded the Digital RF Solutions Corporation in 1986, a fabless semiconductor company using digital CMOS for various radio communications and radar applications. In 1991, Digital RF Solutions merged with Proxim, Inc. to jointly pursue the wireless local area network marketplace using high-speed frequency-hopping spread-spectrum technologies. He is a member of the IEEE, Phi Beta Kappa, Tau Beta Pi, and Eta Kappa Nu and holds more than 12 patents.

Michael McLaughlin (Chapter 22) was a contributor to *Ultra Wideband Systems*. He is chief technical officer at Decawave and has worked for over 20 years in electronic communications. Before founding Decawave, he was the chief technologist at Cornel Electronics and LAKE Datacomms, and while there, he contributed to the V.34, V.90, and V.92 modem recommendations. He invented the technique used in V.92 known as compound precoding. Decawave, along with Freescale and the National Institute of Information and Communications Technology (NICT), are coauthors of DS-UWB, one of the two UWB proposals considered by IEEE802.15.3a. He is a member of the IEEE802.15.4a task group and proposed the preamble and convolutional code selected by the group for that UWB standard. He also helped to define the selected modulation scheme.

Janise Y. McNair (Chapter 14) was a contributor to *Handbook of RF & Wireless Technologies*. She received her BS and MS degrees in electrical engineering from the University of Texas at Austin in 1991 and 1993, respectively, and received her PhD in electrical and computer engineering from the Georgia Institute of Technology in 2000. McNair then joined the faculty in the department of electrical and computer engineering at the University of Florida in Gainesville, Fla., where she currently directs the Wireless and Mobile Systems Laboratory. Her research interests include wireless and mobile networking, specifically medium access control protocols, mobility management, and authentication in wireless multi-network environments. She is a member of the IEEE, Association for Computing Machinery (ACM), Eta Kappa Nu, and Tau Beta Pi.

Douglas B. Miron (Chapters 6 and 7) is the author of *Small Antenna Design*. He received BE and ME degrees in EE from Yale in 1962 and 1963. He received his PhD in EE/Control and Communications from U. Conn. in 1977. He worked in industry from 1963 through 1967, 1970 through 1979 and 1997. He taught at South Dakota State U. from 1979 through 1996, and has been consulting since 1998. He has worked, taught, and published in nearly every major area of electrical engineering. His general interests are in small antennas and RF circuits. He is currently doing research and simulation development for plasmonic applications.

Michael R. Moore (Chapter 16) was a contributor to *Handbook of RF & Wireless Technologies*. He is a research and development engineer in the Engineering and Science Technology Division at Oak Ridge National Laboratory. He holds a BS and MS in electrical engineering from Mississippi State University in Starkville, Miss. His current research expertise includes 16 years in RF instrumentation, health effects, and communications. He has several years of experience in shielding, generating, and modeling electromagnetic fields and their effects. He is an active member of the IEEE SCC28 committee on the biological effects of RF and the IEEE 1451 committee on sensor networking. He currently directs several projects dealing with software radio technologies, specializing in spread-spectrum receivers, and is a communications analyst for the Army's Future Combat Systems (FCS) network, focusing on

system issues, network vulnerability, and combat identification. He has several patents and patents pending in the area of wireless communications.

John T. Moring (Chapter 1) was a contributor to *Handbook of RF & Wireless Technologies*. Moring is a consultant (http://www.moring.net) based in Encinitas, Calif., specializing in wireless technologies. He holds an MS in electrical engineering from the University of Southern California in Los Angeles and teaches communications engineering in various university extension programs. Moring has contributed to emerging technologies throughout his career, including personal computers (1980), spread-spectrum radios (1982), the Internet (1989), and the first Internet-enabled cell phone (1995). Since launching his consultancy in 1997, he has been heavily involved in developing personal area networking technology and wireless location services and is eagerly awaiting the arrival of the Next Big Thing, which is no doubt described in this volume.

Asis Nasipuri (Chapter 15) was a contributor to *Handbook of RF & Wireless Technologies*. He is a professor in the department of electrical and computer engineering at the University of North Carolina at Charlotte. He received his BS in electronics and electrical communication engineering from the Indian Institute of Technology in Kharagpur, India in 1987 and his MS and PhD in electrical computer engineering from the University of Massachusetts at Amherst in 1990 and 1993, respectively. He then joined the Indian Institute of Technology at Kharagpur, India as a faculty member in the Department of Electronics and Electrical Communication Engineering. From 1998 to 2000, he served as a visiting researcher in the Department of Computer Science at the University of Texas at San Antonio. Since 2000, he has been at UNC-Charlotte as an assistant professor of electrical and computer engineering. Nasipuri's research interests include mobile ad hoc and sensor networks, wireless communications, and statistical signal processing. He has published more than 20 research articles on these topics.

Peter Okrah (Chapter 29) was a contributor to *Handbook of RF & Wireless Technologies.* Okrah received his PhD in electrical engineering from Stanford University in Palo Alto, Calif., in 1992. He is with the RF & DSP Infrastructure Division of the Motorola Semiconductor Products Sector in Tempe, Ariz., where he conducts research and development on current and emerging wireless communication applications and technologies. Okrah is a co-recipient of two U.S. patents and has authored or coauthored more than 15 technical papers. He participated as one of the contributing editors of the Release 99 of the 3GPP Specification on Wideband CDMA for Third Generation (3G) cellular system.

Ron Olexa (Chapters 12 and 13) is the author of *Implementing 802.11, 802.16, and 802.20 Wireless Networks*. He is currently President of Horizon Wi-Com, a wireless carrier providing WiMax service to major markets in the Northeast U.S. He is also the owner of Wireless Implementation LLC, a consulting company that has provided technical support and business planning guidance to project as diverse at satellite communications systems, Cellular

network deployments, WiMax and 802.11 hotspot and hotzone implementations. He has previously been CTO at Advanced Radio Telecom and Dialcall, COO of Superconducting Core Technologies, and has held various senior management positions in large wireless communications companies over his 30 year career.

Leonard Pelletier (Chapter 29) was a contributor to *Handbook of RF & Wireless Technologies*. He has been the application support manager for WISD in Tempe, Ariz. for the past eight years and is in charge of providing technical assistance to the RF power amplifier design community. Pelletier holds a BS in electrical engineering from California Polytechnic Institute in Pomona, Calif., and an MBA from Pepperdine University in Malibu, Calif. He is also a California state–registered professional engineer and has been working in the high-power RF arena since 1983.

John Polson (Chapter 26) was a contributor to *Cognitive Radio Technology*. He is an industry expert on military and commercial radio systems. For almost two decades he has served in signal processing algorithm development, Systems Engineering, Principal Investigator, and Product Manager positions at Loral, Lockheed Martin, Motorola, General Dynamics, and Bell Helicopter. He is a highly sought-after and popular speaker; Dr. Polson has taught Mathematics and Computer Science at Park University, Electrical Engineering at New Mexico State University, Computer Security at Webster University, and short courses in Radio Systems and Ultra Wideband technologies for Technology Training Corporation. Dr. Polson's work on Defense Advanced Research Projects Agency (DARPA) programs such as NeXt Generation (XG) Communications, Connectionless Networks (CN), and Variable Red Black Separation Study (VaRBSS) has prompted his research into Cognitive Radio applications and technologies. Additionally, his Net Centric Warfare work for the Armed Reconnaissance Helicopter strengthens his belief that Cognitive Radio applications are on the technology horizon and will soon be in use by consumers and military alike.

Robert D. Poor (Chapter 17) was a contributor to *Handbook of RF & Wireless Technologies*. He is chief technology officer for Ember Corporation in Boston.

Charles Razzell (Chapter 23) was a contributor to *Ultra Wideband Systems*. He received his undergraduate electronics engineering education at the University of Manchester Institute of Science and Technology in the United Kingdom in 1981. Subsequently, he has been involved in various wireless technology projects, usually involving integrated transceivers. His work for Philips has spanned two decades, initially in Europe and later in the United States. He has made regular technical contributions to the IEEE 802.15.3a task group and is an active member of several technical committees of the WiMedia Alliance. He has nine published U.S. patents and is a member of the IEEE Signal Processing and Communications Societies.

Pablo Robert (Chapter 25) was a contributor to *Cognitive Radio Technology*. He earned his BS in Electrical Engineering from Case Western Reserve University in 1996, and his Master of

Science and PhD in Electrical Engineering from Virginia Tech in 1998 and 2003. During his graduate work at Virginia Tech, Dr. Robert received the Bradley fellowship from the Bradley Department of Electrical and Computer Engineering at Virginia Tech, the America Online Wireless Home Networking Technologies fellowship, and the Paul E. Torgersen Graduate Research Excellence award. In 2003, Dr. Robert became an IC Postdoctoral Research Fellow, with a research focus on Software-Defined Radio (SDR). During his fellowship, Dr. Robert started the OSSIE project, a volunteer effort to create an open-source implementation in C++ of the SCA (Software Communications Architecture) Core Framework. Dr. Robert is currently a consultant on SDR and wireless system design.

David Runton (Chapter 29) was a contributor to *Handbook of RF & Wireless Technologies*. He holds a BS in applied physics from Jacksonville University in Jacksonville, Fla., a BS and MS in electrical engineering from Georgia Tech in Atlanta. He has also received an MBA as part of the High Technology Program from Arizona State University in Tempe, Ariz. He is currently the RF systems engineering manager for the RF and DSP Infrastructure Division at the Motorola Semiconductor Products Sector, located in Tempe, Ariz. He has been with Motorola since 1994 in both RF Design and RF Applications engineering.

Hamid R. Sadjadpour (Chapter 31) was a contributor to *Handbook of RF & Wireless Technologies*. He is a professor of electrical engineering at the University of California in Santa Cruz, Calif.

Robert Sutton (Chapter 20) was a contributor to *Ultra Wideband Systems*. He is the president of TDK RF Solutions as well as an acting board member of TDK R&D Corporation. His undergraduate and graduate degrees are from the University of Texas, Austin. Before cofounding the business that ultimately became TDK RF Solutions, he worked in the electromagnetic compatibility laboratory at AT&T Bell Laboratories from 1988 to 1992. Much of his published work covers the topic of small radiating structures and electromagnetic compatibility and coexistence issues.

This page intentionally left blank

CHAPTER 1

A Survey of RF and Wireless Technology

John T. Moring

The last two decades have been the most dynamic in the history of wireless communications.[1] Most notably, mobile voice communications has exploded from a tiny niche market to a part of our daily lives. Building on comparable advances in computers and networking technology, today's wide area and local area wireless systems are poised to take us to the next level of mobile data services, where all the capabilities of the Internet are literally at our fingertips wherever we go.

In this chapter, we briefly review the history of wireless communications, survey today's wireless landscape, and introduce some of the leading-edge topics covered later in this volume.[2]

1.1 A Short History of Wireless Communication

Figure 1.1 shows a time line of the development of wireless communications. We are well into the second century of radio communications. The pioneering work of Faraday, Maxwell, Hertz, and others in the 1800s led to Marconi's wireless telegraph at the turn of the twentieth century. The precursors to mobile radio as we know it have been available since the first transportable voice radios of the 1920s. Radio technology matured in the subsequent decades, with broadcast radio and television, and the portable manpack walkie-talkies of World War II. In the 1940s, cellular technology was conceived, with the ability to divide radio frequency service areas into "cells" to reduce interference and increase capacity. This is the basis for today's wide area voice and wireless local area networking technologies. Within a few years of the first satellite launch in 1957, satellites were being sent into space to act as communication relays.

[1] Coincidently, this period corresponds to the time this author has been employed as a communication engineer. Unfortunately, I can take only partial credit for the amazing advances of this era!

[2] Many thanks to the University of Wisconsin in Madison and Melange Solutions in San Diego, for whom some of this material was originally developed.

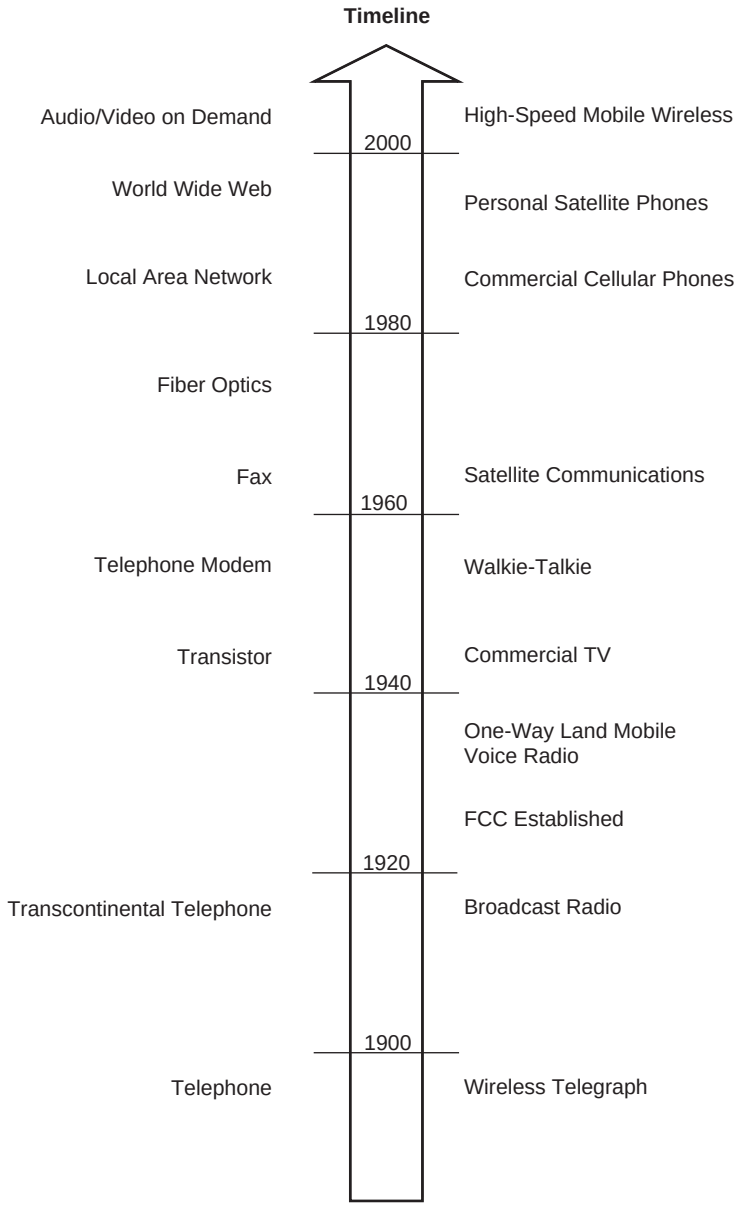

Figure 1.1: The graph indicates general telecommunications advances on the left and wireless-specific advances on the right.

In 1969, the Federal Communications Commission (FCC) allotted portions of the radio frequency spectrum for mobile telephones. In the 1970s the Post Office Code Standardization Advisory Group (POCSAG) numeric paging code was standardized, and AT&T rolled out the first mobile telephone services operating on a cellular system. In 1987, the FCC allowed

the use of new technologies in the 800 MHz cellular spectrum, with the first digital cellular transmissions (code division multiple access [CDMA], time division multiple access [TDMA], and global system for mobile communication [GSM]) tested in the United States shortly thereafter. With the adoption of digital technologies, new features such as voice mail, fax, and short messages have been enabled.

The boom in wireless usage in the 1990s (paralleling the Internet boom) has led to near ubiquitous wireless voice service throughout the United States and in much of the world. Personal wireless data services, exemplified by such technologies as short message service (SMS), wireless application protocol (WAP), ReFlex, Bluetooth, i-Mode, and 802.11, offer a range of mobile data services that are not far behind. For every wireline technology, from serial cable to fiber optics, there is an analogous wireless technology available when it is not feasible or convenient to use a cable connection. Figure 1.2 depicts how rapidly newer technologies grew in the 1990s while the number of wireline telephone installations in homes remained relatively static.

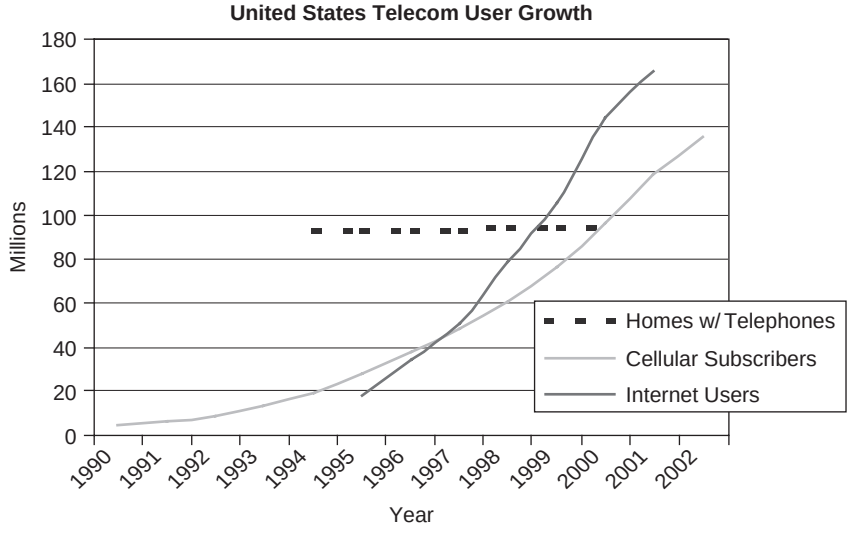

Figure 1.2: United States Telecom User Growth. With voice line penetration in saturation, wireless and Internet users continue to grow. Wireless data usage will follow. (Internet users include the United States and Canada.)

1.2 Where We Are

Today's wireless technologies offer an immense range of capabilities to the user. System throughputs continue to expand, offering the ability to support an increasing number of applications. Wireless communication system availability is also increasing, due to investment in fixed infrastructure, as well as reduced device cost and size.

Figure 1.3 categorizes select wireless technologies, graphed by system throughput and user mobility. Several groupings are identified for convenience. On the left are *Fixed Location* systems, such as point-to-point microwave and stationary satellite systems, which generally operate at high rates (over 1 Mbps) on line-of-sight channels. Near the fixed systems, providing limited mobility over shorter transmission paths but still supporting Mbps data rates, are *Local Area* systems, such as wireless local area networks (802.11) and personal area networks (Bluetooth). Finally, *Wide Area Mobile* systems, such as paging and cellular, provide extended mobility but with relatively limited throughput. These categories are explored in the following section.

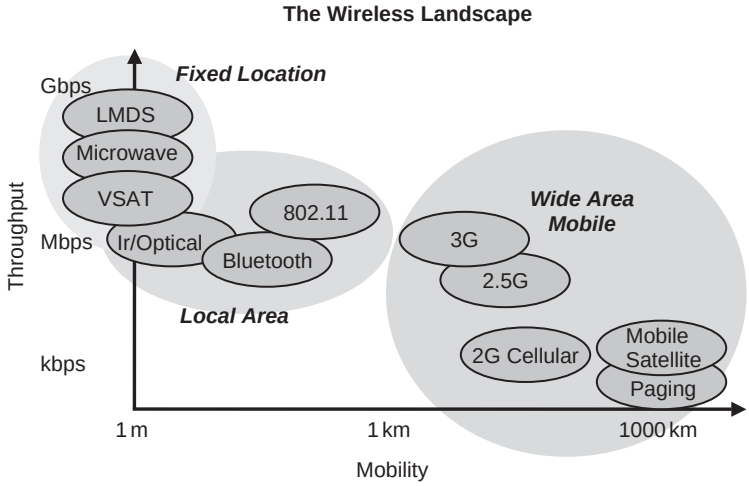

Figure 1.3: Current technologies in the wireless landscape provide a range of choices, from high-bandwidth fixed systems to wide area systems supporting low to moderate data rates.

Before entering a discussion of specific wireless technologies, it is useful to review the relevant characteristics of a generic radio system.

Figure 1.4 illustrates a wireless system, showing a signal sent from the transmitter on the left to the receiver in the center. Other aspects of the environment are shown to highlight the challenges inherent in wireless communications. These challenges are the focus of much research aimed at improving RF communications.

First, even in the best of situations, we have free space *attenuation,* where the signal loses strength at a rate proportional to the square of the distance traveled. This limits the signal propagation distance. The electromagnetic radio waves are further attenuated due to *blockage* by objects (including atmospheric particles) in their propagation paths. Both types of attenuation limit the ability of the receiver to capture and interpret the transmitted signal.

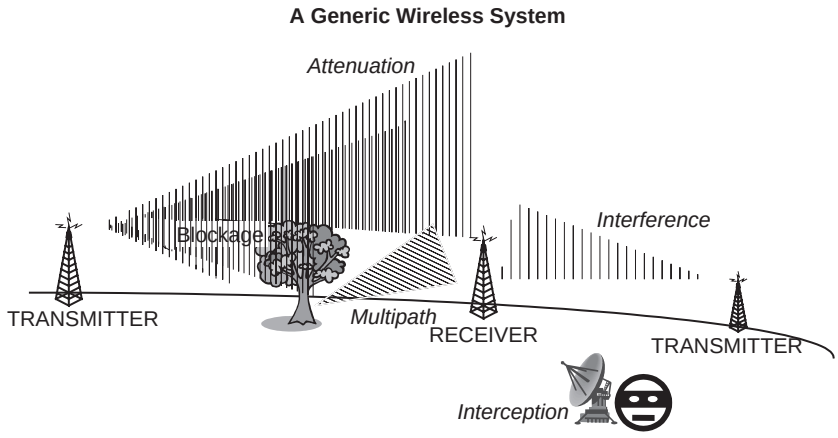

Figure 1.4: A generic wireless system. Inherent weaknesses of the wireless medium are offset by its flexibility and support for mobility.

Additionally, radio signals are subject to reflection, which leads to *multipath* fading, another form of signal loss. A reflected signal, since it travels a longer distance between transmitter and receiver, arrives at the receiver with a time delay relative to a signal following a direct (or shorter reflected) path. Two similar signals, offset in time, may cancel each other out.

Another difficulty facing the receiver operating in the unprotected wireless environment is the possibility of other similar signals sharing the same medium and arriving at the receiver simultaneously with the desired signal, thus causing *interference*. Finally, the unprotected medium also allows the possibility of eavesdropping, or *interception,* where a third party captures the transmitted signal without permission, potentially compromising the privacy of the system's users.

Each of the challenges illustrated in Figure 1.4 identifies an area where wireless communications is at a disadvantage to a comparable wireline communication system. Why, then, are wireless communications so prevalent? Each wireless deployment may have its own design rationale, but two fundamental reasons cover most cases. First, wireless systems provide flexibility in deployment. Whether connecting a laptop PC in a conference room or a pipeline monitor in the Arctic, the setup of a radio connection may be orders of magnitude faster than a wireline connection, due to the fact that no physical connecting media are required. Second, wireless systems can provide the option of mobility. Communicating on the move is very useful, if not critical, to many applications, and this is just not well supported through a wired medium.

Note that some of these "weaknesses" can cleverly be turned to the user's advantage. For example, attenuation and blocking may be leveraged to limit signal propagation and opportunities for eavesdropping.

Having digressed far enough into the advantages and disadvantages of wireless, let us return to the discussion of how the wireless landscape is populated, starting with fixed location systems, and then addressing local area and wide area systems.

1.2.1 Fixed Location Systems

Fixed location systems by their nature can generally support high-gain stationary antennas and connections to the power grid; the resulting high signal-to-noise ratios provide the opportunity to operate at high throughput over long-range line-of-sight paths. Several classes of fixed system are described in the following sections, encompassing both RF and optical as well as terrestrial and space-based systems.

1.2.1.1 Point-to-Point RF

Point-to-point microwave systems typically are used as a substitute for high-speed megabit (T-1, T-3) telecom circuits. They traditionally employ licensed frequencies above 2 GHz and user-owned end equipment. They use highly directional antennas that can span 10 miles and more, given line of sight. (To increase line of sight, systems are often located atop tall buildings and mountaintops.) A recent trend in this domain is toward lower-cost, unlicensed equipment, operating in the 2.4 GHz industrial, scientific, and medical (ISM) or 5 GHz unlicensed national information infrastructure (U-NII) bands.

1.2.1.2 Point to Multipoint

Local multipoint distribution system (LMDS) and multichannel multipoint distribution service (MMDS) are carrier-grade technologies intended for wireless Internet access and general communication services. Spectrum has been allocated for these systems in several super high frequency (SHF) bands, offering tens of megabits per second of throughput. Along these lines, the Institute of Electrical and Electronic Engineers (IEEE) 802.16 working group is developing a family of standards for wireless metropolitan area networks (MANs). The technology provides a competitor to cable modem and DSL access, with additional flexibility. The current telecom slump has slowed the deployment of these systems.

1.2.1.3 VSAT and Other Geosynchronous Satellite Systems

Very small aperture terminal (VSAT) systems are similar to fixed terrestrial multipoint systems, except that instead of a tower- or rooftop-mounted base unit, a satellite transponder is used. A limited number of geosynchronous earth orbit (GEO) satellites circle the equator at 22,236 miles altitude, maintaining a fixed position in relation to a point on the earth. These transponders can be used for high-bandwidth bidirectional signal relay, supporting applications such as data transfer, Internet access, and audio/video signal distribution. Though the ground station antenna is fixed during operation, it is easily deployable, making it well suited for disaster recovery and other temporary situations.

Again, multiple licensed bands are employed. Full satellite channels are often subdivided via multiple access techniques and made available by resellers in the range of 20 kbps to 2 Mbps. According to the Global VSAT Forum,[3] there are over 500,000 VSAT terminals installed worldwide.

1.2.1.4 Free Space Optical

A fairly recent arrival on the scene is free space optical (FSO) communications, which shares characteristics with both point-to-point RF and fiber optic technologies. As in point-to-point systems, a focused signal carries high-throughput bitstreams between two points; as in fiber optics, a laser or light-emitting diode (LED) is used to generate the optical signal that carries the information.

Operating with no spectrum license, and with speeds in excess of 1 Gbps, FSO offers an attractive choice for some backhaul and LAN extension applications. One weakness in today's systems is their susceptibility to optical blockage, particularly from fog.

1.2.2 Local Area Systems

Unlike the fixed systems just considered, local area systems achieve their high throughput via proximity. They generally allow some range of motion on the user's part, providing flexible usage scenarios. The technologies considered here require no spectrum license.

1.2.2.1 Infrared, IrDA

Infrared signals are used for a range of simple control protocols, such as TV remote controls. The Infrared Data Association (IrDA) has standardized multimegabit-per-second data transfers in support of a wide range of usage profiles. Typically, these are very short-range (i.e., inches to feet of separation between units) applications requiring a fairly high degree of directionality between transmitter and receiver. According to IrDA,[4] over 300 million devices support this technology.

1.2.2.2 Bluetooth Personal Area Networks

Operating at 1 Mbps channel rate in the unlicensed 2.4 GHz ISM band, Bluetooth (named for Harald Bluetooth, an ancient Danish Viking king) is intended for low cost and high interoperability. It is variously described as a personal area network (PAN) or a cable replacement technology, and should eventually be routinely embedded in cell phones, computers, PDAs, printers, and a plethora of other products that today require a cable for communications. Over time, more applications (as defined by Bluetooth "Profile" specifications) will be available in such diverse areas as video conferencing and automotive

[3] See http://www.gvf.org.
[4] See http://www.irda.org.

support. With many big names behind it (Bluetooth Promoter companies are 3Com, Agere, Ericsson, IBM, Intel, Microsoft, Motorola, Nokia, and Toshiba) and over 900 distinct Bluetooth[5] products (as of this writing), Bluetooth has a lot of momentum. It also has detractors and competitors.

1.2.2.3 Wireless Local Area Networks

The big news in wireless communications over the last year or two has not been the much-hyped third generation (3G) cellular, but rather wireless local area networking (WLAN) technologies. These technologies (mostly based on the IEEE 802.11 family of standards and marketed under the Wi-Fi banner) operate in unlicensed spectrum, and provide wired LAN extension or replacement. The Wi-Fi family, also known as *Wireless Ethernet,* allows generic applications to operate seamlessly over a transparent layer 1 and 2.

Initially deployed as corporate LAN extensions, their low price, high performance (to tens of Mbps), and ease of operation have made them popular in the home office environment and to a lesser degree as a substitute for traditional point-to-point microwave systems. Additional vertical applications are starting to appear. Some vehicular toll collection systems employ 802.11, and commercial airlines have announced installation of WLANs in their aircrafts for in-flight passenger use. Free access community networks are sprouting in numerous high-tech locales, potentially challenging the business model of established wireless carriers. Wi-Fi's well-publicized security limitations are expected to be solved before they significantly slow adoption of the technology. Over 26 million Wi-Fi devices were expected to ship in 2003 [1].

1.2.3 Wide Area Systems

Wide area mobile systems generally sacrifice throughput for longer propagation paths, user mobility, decreased device size, and increased coverage. Paging and cellular communication systems are prime examples of wide area systems.

1.2.3.1 Paging

Paging was successful for years as a reliable delivery mechanism for short text strings, such as phone numbers. With simplex data delivery, strategically placed high-power transmitters and robust encoding, excellent reliability was achieved. To compete with evolving cell phone services in the 1990s, many paging systems were upgraded to provide two-way transfers and larger message sizes, making them similar in function to the terrestrial packet systems described later in this chapter. Now the Motorola proprietary two-way paging protocol ReFlex is the most widely deployed paging technology.

Faced with the increased coverage and penetration of cellular service, paging subscribership peaked in 1999 [2]. Motorola, the traditional leader among paging manufacturers, announced

[5] See http://qualweb.bluetooth.org.

that it is transitioning away from both one-and two-way paging equipment in favor of advanced cellular products and services [3].

1.2.3.2 Mobile Satellite Services

The 1990s saw the design of a number of LEO and MEO (low and medium earth orbit) satellite systems. Of these, only a few were actually launched, and these have had trouble maintaining financial viability in the face of ever-increasing terrestrial cellular coverage. Two systems provide cellular-like service: Globalstar and Iridium. Others (e.g., Orbcomm) provide two-way paging-like services (though with increased latency, as its LEO satellites are not always overhead). More ambitious systems such as Teledesic await the day when the investment climate may be more propitious.

Successful service providers leverage mobile satellite technology to benefit niche markets. Inmarsat uses a GEO satellite constellation to provide connectivity to maritime and other high-value assets. Omni-Tracs provides vehicular tracking and communications via satellite to the long-haul trucking industry.

1.2.3.3 Specialized Private Systems

Most wide area radio communications—like cellular and paging—are provided as services offered by carriers to the public. A notable exception is military systems, which typically use specialized proprietary designs in restricted frequency bands. Another exception is specialized private systems, used for such applications as voice dispatch and remote asset monitoring. These systems operate in licensed frequency bands and generally consist of several tower sites and many fixed or mobile subscriber units operated by a corporate or government entity. They go by many different names: SMR (specialized mobile radio), MAS (multiaddress system), trunked radio, PMR (private mobile radio), and others. Without the economies of scale of their mass market counterparts, the specialized radio systems are often a generation behind comparable commercial equipment, with many still employing analog modulation, for example, long after cellular has migrated to digital.

1.2.3.4 Terrestrial Packet Systems

Several proprietary systems have been deployed to provide general-purpose packet data services. Mobitex, originally developed by Ericsson, and Ardis, now operated by Motient, provide shared channels operating at about 10 to 20 kbps. Wireless e-mail (similar to two-way paging) has been the dominant application for these systems.

The Ricochet system operates somewhat differently. With low power transceivers mounted on light poles located roughly every quarter mile, the system uses mostly unlicensed spectrum to offer 100-plus kbps Internet access to subscribers. This proprietary system was deployed in 15 or 20 markets before being turned off for financial reasons. At the time of this writing, it is back online in two markets.

1.2.3.5 Cellular

The flagship wireless service is unquestionably cellular. From a few million North American users in the early 1990s, the number of mobile subscribers exceeded the number of fixed telephone subscribers by the end of the 1990s as shown in Figure 1.2. Analog service offered by two carriers per market has given way to high-performance, feature-rich digital services (including SMS, caller ID, three-way calling, etc.), often with four or more carriers per market; additional base stations have been installed to the point where dropped calls and dead spots are exceptions to the rule of ubiquitous connectivity.

North American consumers still have to choose between three or four incompatible second generation digital technologies, though the evolution path points toward two technologies in the coming generation (3G). Within the last year, cellular carriers have deployed their first serious large-scale data offerings, with medium rate (~50 kbps) packet data overlaid on their voice channels. For the first time, wide area consumer data services are available at moderate data rates and low costs. It is yet to be seen exactly how this offering will be used, or how widely it will be accepted.

1.2.4 Applications

We just discussed the current wireless landscape from a technological viewpoint. We can also consider wireless products in terms of the supported applications, such as voice, messaging, private data, and Internet access.

1.2.4.1 Voice

Cellular is the most obvious wireless voice technology. SMR and satellite systems support vertical voice markets, and various technologies (including Bluetooth) are used for short-range cordless telephony. Efforts are underway to support voice services over WLAN technologies.

1.2.4.2 Messaging

Communication via short wireless messages has echoed the popularity of e-mail in a wired environment. Most usage of the Mobitex, Ardis (packet services), and ReFlex (paging) systems today consists of messaging traffic. Terrestrial and satellite voice systems support the SMS, which carries text messages up to about 150 characters over the cellular network. Its successors, enhanced messaging service (EMS) and multimedia messaging service (MMS), now carry enhanced content such as pictures on some networks.

1.2.4.3 Private Data

On an enterprise scale, VSAT and microwave technologies exemplify high-performance data transfer. On a personal scale, technologies such as Bluetooth provide a medium for private data transfer over short ranges. Virtual private network (VPN) is an example of software that allows private communications across a shared infrastructure (e.g., the Internet).

1.2.4.4 Internet Access

Until recently, wireless Internet access involved a 10 kbps cellular channel and a limited web view using the text-based wireless application protocol (WAP) or similar mechanism. Today's digital cellular and wireless LAN services now allow users full web access at reasonable speeds over a wide area. For higher rate fixed access, VSAT services, and in some areas fixed multipoint systems, are available.

1.2.5 Where We Are Going

The advances of the recent decades show no sign of slowing. Despite the current (2003) telecom slump, wireless research and development continues apace. Incremental improvements in all facets of wireless communications should continue for the foreseeable future. Additionally, there are certain ongoing research areas that could potentially provide quantum advances across the wireless landscape.

1.2.5.1 Software Radio

In conventional radios, we see open system interconnect (OSI) Layer 1 (physical) implemented in (mostly analog) hardware, with filters and amplifiers, for example, designed

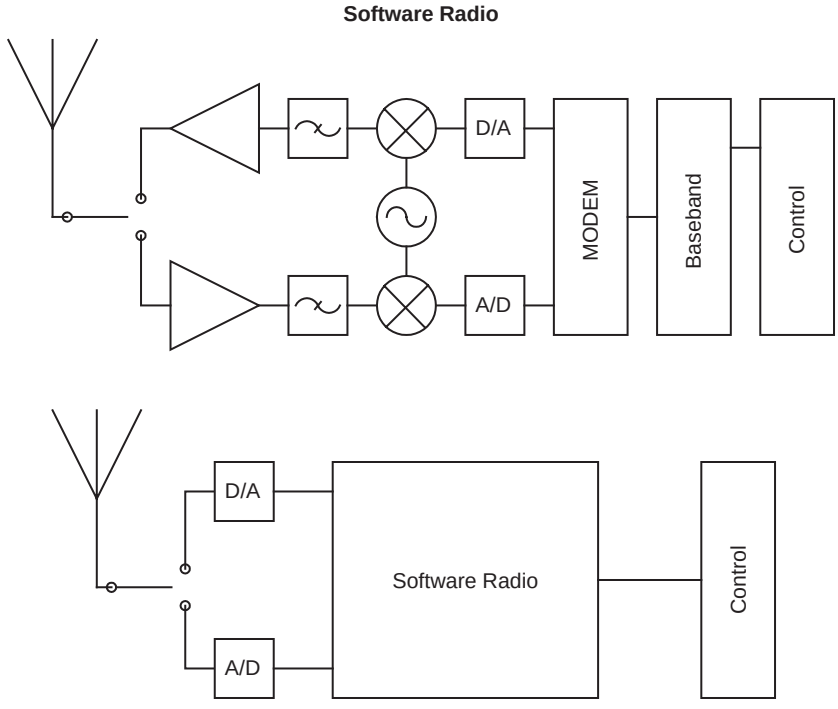

Figure 1.5: The ideal software radio (lower diagram) is much simpler and more flexible than the traditional radio (upper diagram), with its hardware tightly coupled to a specific signal type.

for operation at specific frequencies consistent with the radio's intended usage. Layer 2 (data link) may be implemented in custom digital hardware or a general-purpose digital signal processor; higher layers are usually executed by software/firmware in general-purpose microprocessors. The block diagram of a conventional radio is shown in the top section of Figure 1.5.

The idea behind software radio is to move as much of the radio functionality (including the physical layer) as possible into software. However, performing the high rate sampling and signal processing required for a fully software radio has not yet proven to be commercially feasible. More recently, the related concept of software-defined radio has emerged as an R&D topic. In this case, dynamically reconfigurable logic arrays execute specific computationally intensive functions, such as coding or encryption, as needed. A logic block may be configured as a decoder during reception, then reconfigured as an encoder during the next transmit cycle. The lower section of Figure 1.5 shows a block diagram of a software-defined radio.

For both software radio or software-defined radio, the advantages are similar:

- *Flexibility*—The radio no longer needs to be designed with foreknowledge of the exact characteristics of the target usage.
- *Upgradability*—Operation with a new radio technology can be achieved simply with a new software download.
- *Cost*—Using today's technologies, digital logic gates are inherently less expensive than analog components.
- *Power consumption*—There is potentially more opportunity to optimize for lower power consumption (and therefore longer battery life) for a software/digital function than for analog.

1.2.5.2 Ultrawideband Signals

Ultrawideband (UWB) has been promoted as a technology for applications ranging from high-speed communications to location determination to short-range ground-penetrating imaging. With pulse modulation and bandwidths in excess of 1 GHz, UWB potentially takes the advantages of spread spectrum one step further. The intent is to operate UWB transmitters in an unlicensed mode overlapping licensed frequencies. After significant study, the FCC issued rules allowing limited UWB operation, but questions still remain in the minds of spectrum license holders who are concerned about interference.

1.2.5.3 Smart Antennas

"Smart" antennas have been used for years in specialty applications, especially by the military. There are continuing efforts to develop commercially attractive solutions for applications such as cellular base stations and wireless LAN hot spots. Smart, or phased array, antennas

may be considered an extreme form of antenna diversity. An antenna array is composed of a collection of individual antenna elements, each of which is capable of signal reception (or transmission). A signal arriving at the array will typically be picked up at each element, offset slightly in time. By internally adjusting the phase (time offset) of each received signal and then summing, the antenna pattern is effectively focused on the remote transmitter. Signals arriving from other directions do not benefit from the summing and sink into the noise. The same technique may be used to benefit the transmitted signal as well as the received signal. One of the challenges of the technology is to dynamically adjust the offsets to maintain focus on a remote mobile unit. Figure 1.6 shows a simplified model of smart antenna operation.

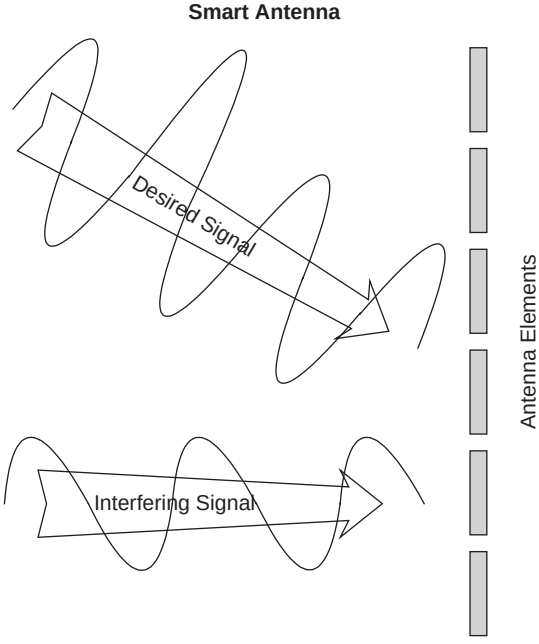

Figure 1.6: Smart antenna. In this simple example, the desired and interfering signals are captured at each antenna element. When aligning the received signals to maximize the desired signal, the offset versions of the interferer tend to cancel each other out.

1.2.5.4 Advanced Networking

There are a number of advances at OSI layers 2 and above that will benefit wireless users, some examples of which are touched on here.

Over the past 15 years, deployment of the Internet protocol (IP) has advanced to where it is now a matter of course to connect from any computer to almost any other computer around the world, and to do it easily and quickly. This expectation also holds true for telephone-to-telephone connectivity. In some respects, mobile telephony is more advanced than IP

networking in that a user can receive a call to his or her unique identifier (telephone number, including the home area code) while roaming to a different market with a different area code. This is not true today in data networking, in which a computer's unique identifier (IP address) is tied to a specific "location" on the network (i.e., a specific router). The situation is addressed by assigning a new IP address as the user reattaches through a different router. This presents limitations to some applications, constraining their ability to maintain a connection as their supporting device moves.

A set of features collectively known as *mobile IP* offers a solution to this problem, providing services to the mobile data use that is comparable to those provided by the mobile telephony infrastructure.

As mentioned earlier, security is one potential weakness of wireless systems. First generation cellular networks were vulnerable to theft of services as well as eavesdropping. These oversights were corrected with authentication and encryption systems built into the second generation systems. Likewise, standards will shortly address the security weaknesses of original IEEE 802.11 wireless LANs.

Another major area of research is in the field of quality of service (QoS). Applications (e.g., voice or video) that work well over dedicated wired links often experience difficulties when faced with the variable delays, channel errors, and throughput inherent in many wireless links. Wireless QoS features will provide a more consistent platform on which to support these applications.

In addition to specific research areas exemplified by those just listed, there are several more general trends that will affect the wireless landscape over the coming years.

1.2.5.5 Increased Throughput

Apart from some low-speed niche applications such as telemetry, each wireless technology is continually pushing for higher data rates. Sophisticated modulation and coding can squeeze more data onto existing channels. Additionally, there is a continuing migration to higher frequencies, where there is more bandwidth and thus the potential for higher throughput. Compare, for example, the newer 802.11a, which supports 54 Mbps on each of up to 12 simultaneous channels at 5 GHz, with 802.11b, which offers 11 Mbps on each of 3 simultaneous channels at 2.4 GHz (under U.S. regulations). Recent news items report that additional spectrum is being proposed to supplement what is already designated for unlicensed use in the 5 GHz band.

1.2.5.6 Increased Access

We have grown to expect near-ubiquitous coverage from our cellular phone carriers. This has been achieved through network tuning and intensive investment in network infrastructure. Next generation technology and business consolidations should provide even

more international roaming capabilities. Where there are several noninteroperable cellular technologies today, there are only two contenders for widespread international deployment in the third generation, and cellular operators are ensuring a much greater degree of compatibility between them. Additionally, the burgeoning growth of public and private Wi-Fi hot spots offers mobile data users another connectivity option. Bluetooth users carry their own personal area network (PAN) around with them wherever they go. And it is expected that satellite services will provide increasing connectivity options for those hard-to-reach remote locales.

1.2.5.7 Ubiquity

Not only is network coverage increasing, but the number of wireless devices is growing at a high rate. The reduced size and price of radios makes it feasible to add wireless capability to almost any device. Advances in supporting technologies, as well as wireless technologies, make radios viable where they never have been before.

- Battery power density continues to improve, reducing the size and increasing the utility of portable devices. Viable alternate power sources are on the horizon.
- User-interface advances (e.g., voice recognition, new display technologies) add convenience and potentially open the door for new applications.
- Integrated circuits continue to double their capabilities every year or two, allowing designers to pack more functions into ever-smaller packages. Newer semiconductor technologies and manufacturing processes provide increased efficiency.
- Processing techniques, such as software-defined radio, scripting and presentation languages (Java 2 Platform, Micro Edition [J2ME], binary runtime environment for wireless [BREW], extensible markup language [XML]), and video compression algorithms, also have the end result of providing more capability—and more configurable capabilities—to our mobile devices.

We are now seeing not only wireless phones and laptop computers, but also radio-connected PDAs, cameras, watches, and cars. Any device that has an embedded microprocessor is a candidate for wireless connectivity. Figure 1.7 illustrates the growth in mobile network access devices.

1.2.5.8 More Applications

The increased availability of network coverage and wireless devices and advances in associated electronics technologies make new applications viable. Mobile voice and mobile text messaging have been wildly popular. The marriage of cameras and wireless opens the door for some form of photo messaging. Cellular carriers (at the behest of the FCC, for safety reasons) are deploying location determination capabilities, some using the global positioning system (GPS). Once these capabilities are in place, a range of new applications beyond public

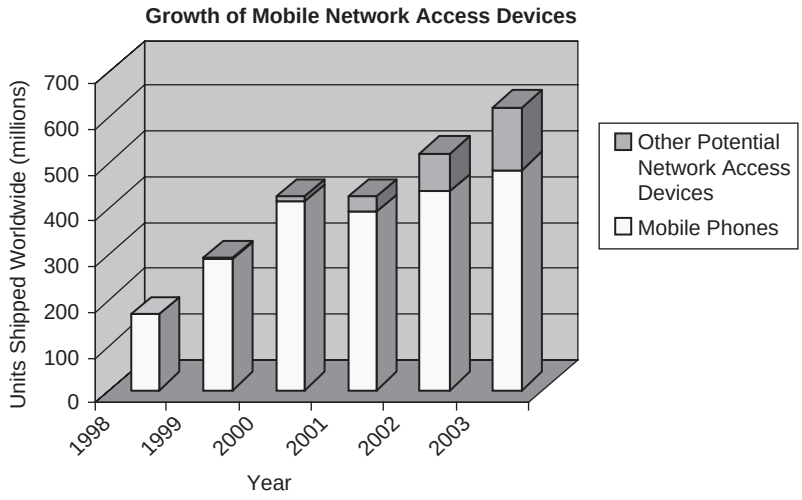

Figure 1.7: Growth of mobile network access devices.[6] "Other" devices include PDAs, handheld and laptop PCs, etc.

safety will be available. Many see electronic gaming as a huge growth area, just now in its infancy.

1.3 Conclusion

The rich history of progress in wireless and RF communication has given us an array of technologies suited to a wide range of applications. We are in a time of explosive growth in wireless technology. Coupled with the Internet content that is now available, the door is open for new applications ranging from telemetry to video. The 1990s saw a proliferation of wireless voice services; now, the wireless data boom will be even more dynamic because the types of devices and content are much more varied.

1.4 References

1. T. Krazit, "Microsoft Joins Home Wi-Fi Announcements," PCWorld.com (http://www.pcworld.com/news/ article/0,aid,10517,00.asp). Accessed September 19, 2002.

2. FCC, *Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services: Sixth Report*, July 17, 2001.

3. Motorola, "Motorola Personal Communications Sector (PCS) Refocuses Messaging Division" (press release), December 3, 2001.

[6] Adapted from the Shosteck Group white paper, *Lessons from Metricom and MobileStar: Success Factors for the Portable Internet Access Market* (January 2002).

CHAPTER 2

Communication Protocols and Modulation

Alan Bensky

In this chapter we take an overall view of the characteristics of the communication system. While these characteristics are common to any wireless communication link, for detail we'll address the peculiarities of short-range systems.

A simple block diagram of a digital wireless link is shown in Figure 2.1. The link transfers information originating at one location, referred to as source data, to another location where it is referred to as reconstructed data. A more concrete implementation of a wireless system, a security system, is shown in Figure 2.2.

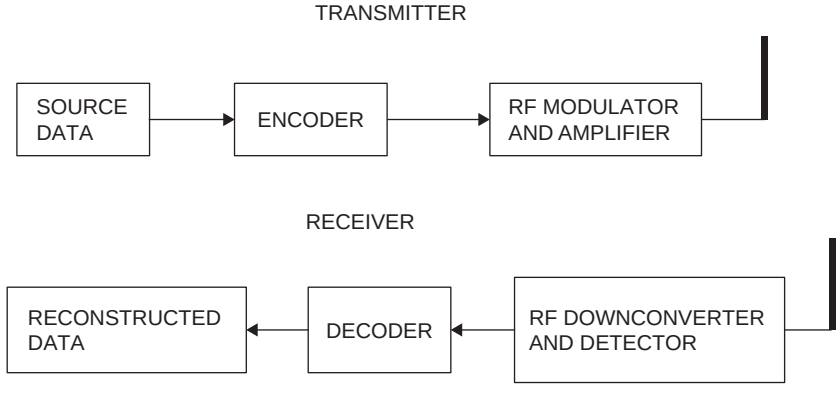

Figure 2.1: Radio communication link diagram.

2.1 Baseband Data Format and Protocol

Let's first take a look at what information we may want to transfer to the other side. This is important in determining what bandwidth the system needs.

2.1.1 Change-of-State Source Data

Many short-range systems only have to relay information about the state of a contact. This is true of the security system of Figure 2.2 where an infrared motion detector notifies the control

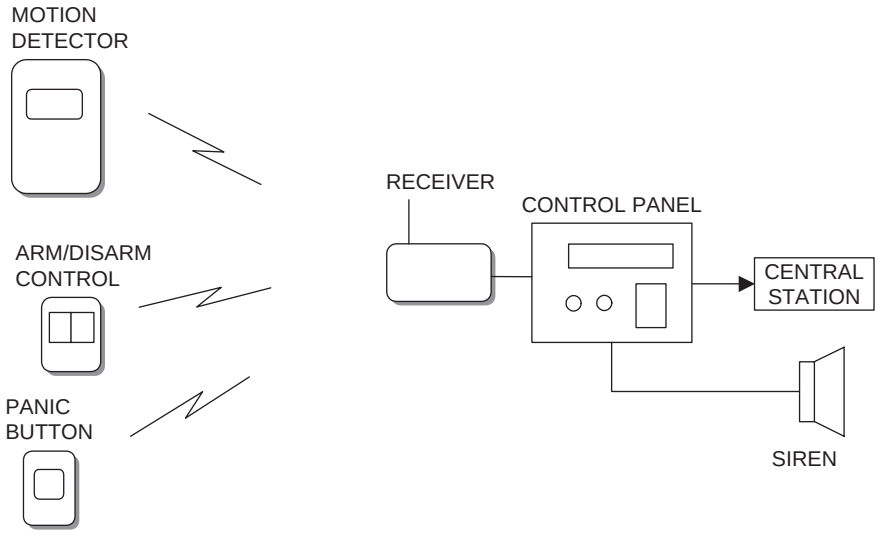

Figure 2.2: Security system.

panel when motion is detected. Another example is the push-button transmitter, which may be used as a panic button or as a way to activate and deactivate the control system, or a wireless smoke detector, which gives advance warning of an impending fire. There are also what are often referred to as "technical" alarms—gas detectors, water level detectors, and low and high temperature detectors—whose function is to give notice of an abnormal situation.

All these examples are characterized as very low bandwidth information sources. Change of state occurs relatively rarely, and when it does, we usually don't care if knowledge of the event is signaled tens or even hundreds of milliseconds after it occurs. Thus, required information bandwidth is very low—several hertz.

It would be possible to maintain this very low bandwidth by using the source data to turn on and off the transmitter at the same rate the information occurs, making a very simple communication link. This is not a practical approach, however, since the receiver could easily mistake random noise on the radio channel for a legitimate signal and thereby announce an intrusion or a fire when none occurred. Such false alarms are highly undesirable, so the simple on/off information of the transmitter must be coded to be sure it can't be misinterpreted at the receiver.

This is the purpose of the encoder shown in Figure 2.1. This block creates a group of bits, assembled into a frame, to make sure the receiver will not mistake a false occurrence for a real one. Figure 2.3 is an example of a message frame. The example has four fields. The first field is a preamble with start bit, which conditions the receiver for the transfer of information and tells it when the message begins. The next field is an identifying address. This address is unique to the transmitter, and its purpose is to notify the receiver from where or from what unit the message is coming. The data field follows, which may indicate what type of event

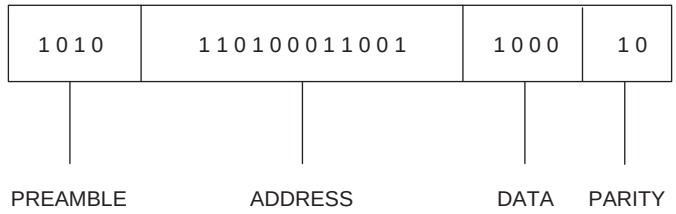

Figure 2.3: Message frame.

is being signaled, followed, in some protocols, by a parity bit or bits to allow the receiver to determine whether the message was received correctly.

2.1.1.1 Address Field

The number of bits in the address field depends on the number of different transmitters there may be in the system. Often the number of possibilities is far greater than this, to prevent confusion with neighboring, independent systems and to prevent the statistically possible chance that random noise will duplicate the address. The number of possible addresses in the code is 2^{L1}, where $L1$ is the length of the message field. In many simple security systems the address field is determined by dip switches set by the user. Commonly, 8 to 10 dip switch positions are available, giving 256 to 1,024 address possibilities. In other systems, the address field, or device identity number, is a code number set in the unit microcontroller during manufacture. This code number is longer than that produced by dip switches and may be 16 to 24 bits long, having 65,536 to 16,777,216 different codes. The longer codes greatly reduce the chances that a neighboring system or random event will cause a false alarm. On the other hand, the probability of detection is lower with the longer code because of the higher probability of error. This means that a larger signal-to-noise ratio is required for a given probability of detection.

In all cases, the receiver must be set up to recognize transmitters in its own system. In the case of dip-switch addressing, a dip switch in the receiver is set to the same address as in the transmitter. When several transmitters are used with the same receiver, all transmitters must have the same identification address as that set in the receiver. In order for each individual transmitter to be recognized, a subfield of two to four extra dip-switch positions can be used for this differentiation. When a built-in individual fixed identity is used instead of dip switches, the receiver must be taught to recognize the identification numbers of all the transmitters used in the system; this is done at the time of installation. Several common ways of accomplishing this are

(a) *Wireless "learn" mode.* During a special installation procedure, the receiver stores the addresses of each of the transmitters that are caused to transmit during this mode;

(b) *Infrared transmission*. Infrared emitters and detectors on the transmitter and receiver, respectively, transfer the address information;

(c) *Direct key-in*. Each transmitter is labeled with its individual address, which is then keyed into the receiver or control panel by the system installer;

(d) *Wired learn mode*. A short cable temporarily connected between the receiver and transmitter is used when performing the initial address recognition procedure during installation.

2.1.1.2 Advantages and Disadvantages of the Two Addressing Systems

Dip switch

Advantages	Disadvantages
Unlimited number of transmitters can be used with a receiver.	Limited number of bits increases false alarms and interference from adjacent systems.
Device can be used with commercially available data encoders and decoders.	Device must be opened for coding during installation.
Transmitter or receiver can be easily replaced without recoding the opposite terminal.	Multiple devices in a system are not distinguishable in most simple systems.
	Control systems are vulnerable to unauthorized operation, since the address code can be duplicated by trial and error.

Internal fixed code identity

Advantages	Disadvantages
Large number of code bits reduces possibility of false alarms.	Longer code reduces probability of detection.
System can be set up without opening transmitter.	Replacing transmitter or receiver involves redoing the code learning procedure.
Each transmitter is individually recognized by receiver.	Limited number of transmitters can be used with each receiver.
	Must be used with a dedicated microcontroller. Cannot be used with standard encoders and decoders.

2.1.2 Code-Hopping Addressing

While using a large number of bits in the address field reduces the possibility of false identification of a signal, there is still a chance of purposeful duplication of a transmitter code to gain access to a controlled entry. Wireless push buttons are used widely for access control to vehicles and buildings. There are radio receivers, popularly called "code grabbers,"

that receive the transmitted entry signals and allow retransmitting them for fraudulent access to a protected vehicle or other site. To counter this possibility, addressing techniques were developed that cause the code to change every time the push button is pressed, so that even if the transmission is intercepted and recorded, its repetition by a would-be intruder will not activate the receiver, which is now expecting a different code. This method is variously called code rotation, code hopping, or rolling code addressing. In order to make it virtually impossible for a would-be intruder to guess or try various combinations to arrive at the correct code, a relatively large number of address bits are used. In some devices, 36-bit addresses are employed, giving a total of over 68 billion possible codes.

In order for the system to work, the transmitter and receiver must be synchronized. That is, once the receiver has accepted a particular transmission, it must know what the next transmitted address will be. The addresses cannot be sequential, since that would make it too easy for the intruder to break the system. Also, it is possible that the user might press the push button to make a transmission but the receiver may not receive it, due to interference or the fact that the transmitter is too far away. This could even happen several times, further unsynchronizing the transmitter and the receiver. All of the code-hopping systems are designed to prevent such unsynchronization.

Following is a simplified description of how code hopping works, aided by Figure 2.4.

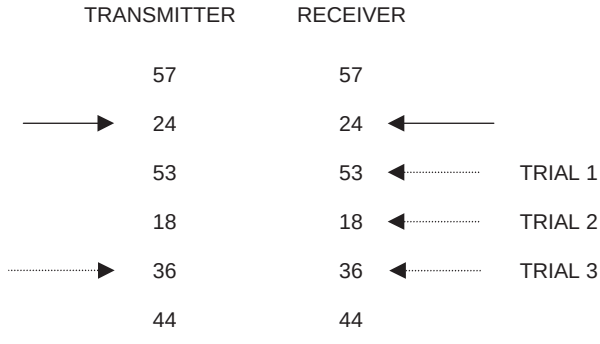

Figure 2.4: Code hopping.

Both the receiver and the transmitter use a common algorithm to generate a pseudorandom sequence of addresses. This algorithm works by manipulating the address bits in a certain fashion. Thus, starting at a known address, both sides of the link will create the same next address. For demonstration purposes, Figure 2.4 shows the same sequence of two-digit decimal numbers at the transmitting side and the receiving side. The solid transmitter arrow points to the present transmitter address, and the solid receiver arrow points to the expected receiver address. After transmission and reception, both transmitter and receiver calculate their next addresses, which will be the same. The arrows are synchronized to point to the same

address during a system setup procedure. As long as the receiver doesn't miss a transmission, there is no problem, since each side will calculate an identical next address. However, if one or more transmissions are missed by the receiver, when it finally does receive a message, its expected address will not match the received address. In this case it will perform its algorithm again to create a new address and will try to match it. If the addresses still don't match, a new address is calculated until either the addresses match or a given number of trials have been made with no success. At this point, the transmitter and receiver are unsynchronized, and the original setup procedure has to be repeated to realign the transmitter and receiver addresses.

The number of trials permitted by the receiver may typically be between 64 and 256. If this number is too high, the possibility of compromising the system is greater (although with a 36-bit address a very large number of trials would be needed for this) and with too few trials, the frequency of inconvenient resynchronization would be greater. Note that a large number of trials take a lot of time for computations and may cause a significant delay in response.

Several companies make rolling code components, among them Microchip, Texas Instruments, and National Semiconductor.

2.1.3 Data Field

The next part of the message frame is the data field. Its number of bits depends on how many pieces of information the transmitter may send to the receiver. For example, the motion detector may transmit three types of information: motion detection, tamper detection, or low battery.

2.1.3.1 Parity Bit Field

The last field is for error detection bits, or parity bits. As discussed later, some protocols have inherent error detection features so the last field is not needed.

2.1.3.2 Baseband Data Rate

Once we have determined the data frame, we can decide on the appropriate baseband data rate. For the security system example, this rate will usually be several hundred hertz up to a maximum of a couple of kilohertz. Since a rapid response is not needed, a frame can be repeated several times to be more certain it will get through. Frame repetition is needed in systems where space diversity is used in the receiver. In these systems, two separate antennas are periodically switched to improve the probability of reception. If signal nulling occurs at one antenna because of the multipath phenomena, the other antenna will produce a stronger signal, which can be correctly decoded. Thus, a message frame must be sent more often to give it a chance to be received after unsuccessful reception by one of the antennas.

2.1.3.3 Supervision

Another characteristic of digital event systems is the need for link supervision. Security systems and other event systems, including medical emergency systems, are one-way links.